CA2389472

Publication Title:

METHOD FOR FILTERING EMAIL SPAM

Abstract:

Abstract of CA 2389472

(A1) Software and system that provides an effective means of limiting Unsolicited Commercial Email (A.K.A. "spam") without the risk of blocking legitimate email and without th e need for the user to configure complex software, write filtering rules, maintain lists of email addresses, or change the way they currently retrieve, read, compose and send email. The invention includes a central database called the "Registry" that contains information about email address es that is provided directly and indirectly by the senders and receivers of email messages and that is derived from the process of users sending and receiving email messages; a centralized collaborative rating process that uses information contained in the Registry to evaluate and rate each email address; an email "ratings server" that contains rating values for email addresses; and "filtering software" that filters email messages based on the users preferences and currently assigned address rating values provided by the ratings server.

---

(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

(11) CA 2 389 472 (13) A1

(40) 17.12.2003
(43) 17.12.2003

(12)

(21) 2 389 472

(22) 17.06.2002

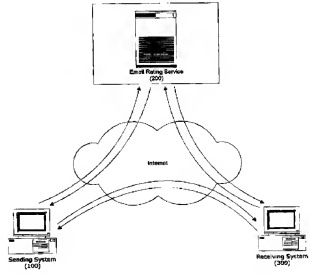
(51) Int. Cl.[7]: H04L 12/54, H04L 12/16

(71)
WARRIS, RON W.,
2211 16A St. S.W., CALGARY, A1 (CA).
RAE, DONNA M.,
281 Big Springs Drive, AIRDRIE, A1 (CA).
WOYNARSKI, SCOTT P.,
516 - 3600 Brenner Drive, CALGARY, A1 (CA).

(72)
WARRIS, RON W. (CA).
RAE, DONNA M. (CA).
WOYNARSKI, SCOTT P. (CA).

(54) METHODE DE FILTRAGE DE POURRIEL
(54) METHOD FOR FILTERING EMAIL SPAM

(57)
Software and system that provides an effective means of limiting Unsolicited Commercial Email (A.K.A. "spam") without the risk of blocking legitimate email and without the need for the user to configure complex software, write filtering rules, maintain lists of email addresses, or change the way they currently retrieve, read, compose and send email. The invention includes a central database called the "Registry" that contains information about email addresses that is provided directly and indirectly by the senders and receivers of email messages and that is derived from the process of users sending and receiving email messages; a centralized collaborative rating process that uses information contained in the Registry to evaluate and rate each email address; an email "ratings server" that contains rating values for email addresses; and "filtering software" that filters email messages based on the users preferences and currently assigned address rating values provided by the ratings server.



Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2389472 A1 2003/12/17

(21) 2 389 472

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2002/06/17

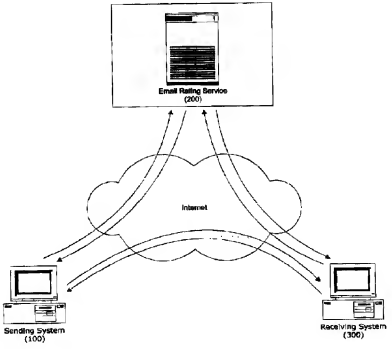
(41) Mise à la disp. pub./Open to Public Insp.: 2003/12/17

(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 12/54, H04L 12/16

(71) Demandeurs/Applicants:
WARRIS, RON W., CA;
WOYNARSKI, SCOTT P., CA;
RAE, DONNA M., CA

(72) Inventeurs/Inventors:
WARRIS, RON W., CA;
WOYNARSKI, SCOTT P., CA;
RAE, DONNA M., CA

(54) Titre : METHODE DE FILTRAGE DE POURRIEL
(54) Title: METHOD FOR FILTERING EMAIL SPAM



(57) Abrégé/Abstract:
Software and system that provides an effective means of limiting Unsolicited Commercial Email (A.K.A. "spam") without the risk of blocking legitimate email and without the need for the user to configure complex software, write filtering rules, maintain lists of email addresses, or change the way they currently retrieve, read, compose and send email. The invention includes a central database called the "Registry" that contains information about email addresses that is provided directly and indirectly by the senders and receivers of email messages and that is derived from the process of users sending and receiving email messages, a centralized collaborative rating process that uses information contained in the Registry to evaluate and rate each email address, an email "ratings server" that contains rating values for email addresses, and "filtering software" that filters email messages based on the users preferences and currently assigned address rating values provided by the ratings server.

METHOD FOR FILTERING EMAIL SPAM

ABSTRACT

Software and system that provides an effective means of limiting Unsolicited Commercial Email (A.K.A. "spam") without the risk of blocking legitimate email and without the need for the user to configure complex software, write filtering rules, maintain lists of email addresses, or change the way they currently retrieve, read, compose and send email. The invention includes a central database called the "Registry" that contains information about email addresses that is provided directly and indirectly by the senders and receivers of email messages and that is derived from the process of users sending and receiving email messages; a centralized collaborative rating process that uses information contained in the Registry to evaluate and rate each email address; an email "ratings server" that contains rating values for email addresses; and "filtering software" that filters email messages based on the users preferences and currently assigned address rating values provided by the ratings server.

BACKGROUND OF THE INVENTION

Electronic mail (more commonly referred to as "email") has introduced an extremely low cost means for people to communicate with others around the world using the Internet. However an unfortunate side effect of this new, low cost communications medium is the distribution of electronic marketing messages commonly known as "spam" or "junk email".

More properly referred to as Unsolicited Commercial Email ("UCE") or Unsolicited Bulk Email ("UBE"), spam includes any unsolicited or unwanted email message that is sent to Internet users. Such unsolicited email is often sent to millions of email addresses at the same time, and often from a single email address that is valid for only a short period of time.

Many people consider spam as more than just a nuisance as it in effect 'steals' resources from businesses, Internet Service Providers ("ISP's") and individuals. Resources most affected by spam theft include: 1.) bandwidth that is lost handling unwanted email; 2.) time that is lost by employees sorting and deleting spam; 3.) computing resources that are consumed by ISP's and businesses trying to identify and filter spam, etc.

Spam also increases the risk of accidentally deleting or overlooking important messages while sorting spam from legitimate messages. Spam frequently contains objectionable, fraudulent, or dangerous content, such as pornography, illegal pyramid schemes and other financial scams.

Even more significant is the increased security risk that spam represents as it is commonly used to distribute destructive viruses, software code (Java applets, JavaScript, ActiveX, etc.) and worms, which are included in the email message either as attachments or active content, that when opened can wreak havoc on the users computer by deleting files, modifying information, turning off security protocols, and so on.

Consequently, there is a need for an effective method that automatically identifies and controls the delivery of unwanted email to users' in-boxes, without impacting the users normal email processes and without any possibility of inadvertently labeling legitimate email as spam.

DESCRIPTION OF PRIOR ART

Previous attempts in the prevention of spam have included: 1.) scanning each incoming email message for key words and phrases that are typically found in spam message; 2.) preventing the delivery of email messages from specific Internet domains and IP addresses that have been identified as sources of spam email; 3.) limiting email messages to specific email addresses (whitelisting), and; 4.) limiting email messages from specific email addresses (blacklisting). The most advanced filtering methods often use a combination of the above techniques backed up with a human review process.

By far the most common spam control technique is scanning each incoming email message for key words or phrases that are typically found in spam messages. More sophisticated products use fuzzy logic and a scoring system to try and detect spam. Simpler products simply use a list of known words and phrases to try and filter out spam messages. In all cases this approach to filtering spam suffers from two major problems. The first is the potential of misidentifying a legitimate message as spam, representing a serious risk for business users if the filter accidentally deletes an important email message. And the second is the need to download the entire email message from the Email Service Provider ("ESP") before it can be determined if the message is spam or not, thereby wasting expensive bandwidth and computing resources on spam.

Domain and IP level filtering techniques are commonly use by ISPs, ESPs and commercial users who often rely on lists of known sources of spam email that are compiled and maintained by non-profit organizations such as the Mail Abuse Prevention System ("MAPS"). MAPS maintains and operates the Realtime Blackhole List ("RBL") – a list of known networks that allows spammers to send unsolicited email messages. While domain and IP filtering can be very effective in blocking unwanted spam, they often inadvertently block legitimate email messages from individuals and organizations that are part of the blocked domain or IP address.

Whitelisting and blacklisting of email addresses are also commonly used spam-filtering techniques typically incorporated into the software that allows the user to compose, send, retrieve and read email. Additionally there are third party add-on programs that offer the user the ability to create email address filtering lists. Whitelisting does work reasonably well, but requires the user to continuously maintain their list of email addresses that they wish to receive email from. Blacklisting on the other hand has proven to be a relatively ineffective technique as the senders of spam messages often use a different (and often invalid) reply addresses for every piece of email they send out, making it virtually impossible to keep a blacklist up-to-date.

Very advanced filtering systems use a multi-pronged approach to filtering email backed up by a human review process and have proven to be very effective. However they are very expensive to implement and operate and are usually well beyond the reach of individuals and smaller ISPs, ESPs and businesses.

Therefore it is the objective of the present invention to provide an effective, low cost means of limiting spam email without the risk of blocking legitimate email, and without the need for the user to change their email handling procedures or behavior, maintain complex software, write and maintain word/phrase filtering rules, or create and maintain whitelists and blacklists of email addresses.

SUMMARY OF THE INVENTION

In accordance with the present invention, a centralized "Registry" (201) maintains a database (206) of email addresses, which are provided either by the Senders of email messages (100) using an email registration process (208), or by an email proxy (102, 302) in instances where an email proxy (102,

302) has submitted a request to a "Ratings Server" (202) for a rating for the email address and the address has not yet been registered by the owner, or in instances where a user of the email proxy software (102, 302) has added the email address to their personal list of email addresses that they will always accept email from (the "GOlist"), or their personal list of email addresses that never want to receive email from (the "STOPlist").

Each email address maintained by the Registry is assigned a spam rating value (205) using a rules driven, Collaborative Rating Process ("CRP") (204). Rules are collaborative in nature in that they use information that is provided directly and indirectly by the senders and receivers of email messages along with operational information that is derived from the process of users receiving email messages when they have the email proxy software (302) installed on their computer. Assigned rating values are in turn sent to an email address ratings server (202) which are in turn used by a filtering process (303) that is part of the email proxy software (302) that is installed on the users computer (300) and that uses the currently assigned spam rating value and the users preferred filtering settings to determine whether an email message should be delivered to the users email software (301) or if the message should be detained by the proxy as possible spam. (306)

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic diagram showing the main components of the present invention;

FIG. 2 is a detailed schematic diagram that shows the functionality of the present invention;

FIG. 3 is a functional block diagram of the preferred embodiment of the present invention;

FIG. 4 is a flow diagram that describes the installation of the proxy software onto the users computer;

FIG. 5 & 6 are flow diagrams that describe the email address registration process;

FIG. 7 is a flow diagram that describes the use of an optional GOlist;

FIG. 8 is a flow diagram that describes the use of an optional STOPlist;

FIG. 9 is a flow diagram that describes the process of updating the registry with information from GOlists and STOPlists;

FIG. 10-12 are flow diagrams that describes how the proxy retrieves and uses address ratings from the rating server to filter email for the user, and;

FIG. 13 is a flow diagram that describes the email address registration process.

DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 is a schematic diagram representing the three main components of the fully functional spam filtering process, including the Sender (100) the Email Rating Service (200) and the Receiver (300). The Sender wants to send email to the Receiver. The Receiver wants to ensure that the email being sent is not spam. The Email Rating Service provides email address rating information to the Receiver. The Receiver in turn uses this information to determine if the email sent by the Sender may be spam and takes the appropriate action.

It should be noted that the role of the Sender (100) and Receiver (300) may be reversed. In addition Senders and Receivers could represent individuals or other entities such as a business, ISP or ESP. It should also be noted that the sending or receiving systems may be a personal computer ("PC") or a server used to queue, send, receive and hold email. It should also be noted that there may be one-to-one, one-to-many and many-to-one relationships between Sending and Receiving systems.

FIG. 2 is schematic diagram that provides a more detailed overview of how the filtering process works. Lets begin with the sender (100) who wishes to send an email message to the receiver. (300) The sender composes the message using their preferred email software (101) and sends the email message via the Internet (1) using their preferred ESP. The email message is routed by the Internet (2) to the receivers ESP where the message is held until the receivers email proxy asks the ESP for the header portion of all the email messages that are waiting to be delivered to the receiver. (4,3) (The "header" portion of an email message contains the postal information of the message, such as the recipient, the sender, the subject, etc. Headers also contain message routing instructions and other technical information that is used to direct an email message to its destination.) Normally the receivers preferred email software downloads the entire email message from the receivers ESP, but

if the receiver has installed the email proxy software (302) onto their system, then the proxy (302) manages the retrieval of the receivers email on behalf of the receivers email software.

Once the proxy has downloaded the email headers from the ESP (2,5) it parses out the senders email address and if the user has created a GOlist or STOPlist, compares the email address to email addresses that are on the users GOlist and STOPlist. If the email address is in the users GOlist, then the proxy sends a request to the ESP to download the entire message (5,3,2,4) and then passes the message on to the receivers preferred email software program. If the email address is in the users STOPlist, then depending on how the receiver has configured the proxy software (302), the proxy either deletes the message header from the receivers computers and instructs the ESP to delete the entire email message from it's server, or it places the message header in a "detained" list of email messages so that the receiver can review the message header information at their leisure and decide if they want to retrieve the entire message from the ESP, or delete the message without ever reading it. The definition and use of GOlists and STOPlists by the receiver is totally optional and are only provided as a convenience and an added level of filtering control for the receiver. GOlists and STOPlists ARE NOT required for the filtering process to work effectively.

If the email address is not on either the receivers GOlist or STOPlist, then the proxy sends a request via the Internet (4,6) to the address Rating Server (202) for the current spam rating of the email address. If the address has been assigned a rating value, then the address Rating Server forwards the address rating back to the receiver's proxy (302) via the Internet (7,5). The receiver's proxy then uses the rating provided by the address Rating Server to determine what to do with the message. If the returned rating is higher then the minimum required rating set by the receiver for delivery of the message to the receiver's inbox, then the message header is placed in the receiver's detained list of messages (306) so that the receiver can review the message header information at their leisure and decide if they want to retrieve the entire message from the ESP, or have the message deleted. Additional processes can be provided that will result in the email headers being automatically deleted from the detained message list (306) if the receiver takes no action after a preset period of time.

If the returned rating is lower then the minimum required rating set by the receiver for delivery of the message to the receiver's inbox, then the proxy sends a request to the ESP to send the entire

email message to the proxy. (4,2,3,5) After the entire message has been retrieved by the proxy, it is then automatically forwarded to the receivers preferred email software.

If however the address Rating Server returns a value that indicates that the senders email address does not have an assigned rating value, then the receivers proxy places the email headers into the receivers detained list (306) and automatically sends a pre-composed email message to the sender via the Internet (4,8) on behalf of the receiver. The pre-composed email message will typically include a personal message from the receiver as well as information that the sender will need to register their email address with the Registry (201) before their email will be delivered to the receiver. (300) The registration information included in the email message will direct the sender of the original email message to a web based email registration process (1,10) (208) that will ask the sender for the email address they wish to register and what kind of email will be sent using that email address. To protect the privacy of the sender no other information other than the email address and what the address is used for is requested by the email address registration process. To prevent spammers from automatically registering hundreds or even thousands of email addresses from which they could send spam, the web-based registration process includes a non-machine readable tag that the registrant must manually enter into the registration form. As a further anti-spam deterrent, all address registration requests must be verified by the address owner using a double opt-in process, wherein the registration request is verified by emailing a confirmation message to the provided email address requiring the address owner to respond to the registration request by entering a randomly generated registration code that is included in the registration confirmation email message into a web-page so that the registration process can confirm that the email address is valid, and that the owner of the email address does indeed wish to have the address registered. As an alternative method to keying in a randomly generated code, the email message could include a URL that includes a randomly generated code. When the user goes to the URL with their browser the coded URL will confirm to the registration process that the email address is valid and that the address owner wishes to have the address registered.

Once the registration process is completed, then the Email Rating Service (200) will assign a rating value to the email address using a rules driven, Collaborative Rating Process ("CRP") (204). The CRP uses information accumulated about each email address that may include (but is not limited to): 1.) when the email address was registered; 2.) the number of rating requests received for each email

address; 3.) the date and time that each rating request was made for the email address; 4.) the number of GOlists and STOPlists that the email address is currently on; 5.) the number of spam complaints received about the email address; 6.) the type of email that the email address has been registered to send (personal mail, newsletters, opt-in email, email based discussions, etc.); 7.) the IP address that the email address was registered from; 7.) the HTTP header information recorded from the address owners browser when they confirmed their registration request; 8.) how the email address was added to the Registry, i.e.: by the address owner or from a GOlist or STOPlist; 9.) the history of rating changes for the email address, and ; 10.) the header information from received email messages, etc. In the case of a newly registered email address the amount of information available is somewhat limited for that address, so the rating value assigned by the system may reflect that lack of information.

Email addresses may be included in the Registry (201) even if they have not been registered by the address owner. An address can be added to the Registry when a proxy makes a request for an address rating and the address has not been previously entered into the Registry. It can be added to the Registry when a proxy user adds the email address to either their GOlist or STOPlist. Or it may be added as the result of someone complaining about receiving spam email from the email address. In all instances, email addresses that have not been registered by the address owner are processed by the CRP and assigned a rating that can be used by the receiver's proxy to filter email sent to the receiver.

Once the CRP has determined and assigned a rating for the email address, the email address and associated rating value is passed (9) to the Address Rating Server ("Rating Server") (202). The next time that the receivers proxy checks for a rating assignment for email addresses of messages that have been placed in the detained list, (306) then Rating Server returns the newly assigned rating and the proxy determines how to handle the email message based on how the receiver has configured their filtering preferences.

FIG. 3 is a functional block diagram of the preferred embodiment of the system as shown in FIG. 1 and 2. In this embodiment each of the Sending (100) and Receiving (300) system includes a Message Filtering Module (103, 303), Configuration Module (104, 304), Address Management Module (105, 305), Detained Messages Module (106, 306), and Registration Request Module (107,

307), all of which may communicate with each other within the proxy software. In the preferred embodiment each of the modules are implemented as software, but can also be implemented as hardware and/or firmware. Examples of sending and receiving systems (100, 300) include desktop computers, portable computers, servers, PDAs, wireless devices and other digital devices.

The Email Rating Service (200) includes the email Registry (201) and the Ratings Server (202).

The email Registry (201) includes the following modules: Collaborative Rating Module (204), Ratings Maintenance Module (205), Address Information Storage (206), Email Registration Module (208), Client Registration Module (209), Messaging Module (210), and the Administration Module (207). All of the email Registry modules may communicate with each other. In the preferred embodiment each of the modules are implemented as software, but can also be implemented as hardware and/or firmware. An example of an implementation of an Email Registry (201) would include server software running UNIX, Linux, Windows NT/2000/XP or Sun Solaris systems.

The system outlined in Fig. 3 generally operates in a manner described by the flow charts illustrated in Fig. 4 to Fig 13, which will be described below.

Turning now to Fig 4., the filtering process begins with a user who wants to reduce or eliminate the volume of spam that they receive. They may learn about this new registration based filtering process from friends and acquaintances who have already installed the proxy onto their personal computers, or from a registration request message that they received from a user of the proxy software (102, 302) that they have sent an email message to. As a result they decide that they would like to try the filter and download the software from any one of the many software distribution hubs on the Internet, or directly from the Email Rating Service's own website.

During the installation process (405) the user will be asked to provide their email address to confirm that the address has been properly registered with the central Registry. (201) (410) To determine the current registration status of the users email address, the installation process sends a registration confirmation request to the Registry. (201, 210) (415) If the email address has not been registered by the address owner, then the Registry (201, 210) returns a not registered message and the installation process directs the user to the registration website that is part of the email registration module. (208) (450) While the user is not required to complete the entire double opt-in registration process before

they can finish installing the proxy software, (102, 302) they are required to initiate the registration process by completing and submitting the email address registration form. After the user has initiated the email registration process the installation of the proxy software (102, 302) continues. (425) After the software has been installed a registration process (430) is initiated that includes sending a GUID ("Globally Unique Identifier") that was generated during the installation process to the Registry (201) uniquely identifying each installation of the software. Additional information about the user of the software may also be gathered and sent to the Registry (201). Once the proxy (102, 302) has been registered, the installation process (435) continues with the user being provided with the option (440) to configure the software (104, 304) using a step-by-step wizard style configuration process, (445) or an advanced software configuration process. (455)

Figs. 5 & 6 provides a detailed flow diagram describing the email address registration process. The process begins when a person is directed to a web page that contains an email address registration application form. A person may be directed to this form during the course of installing the proxy software (102, 302) (400); as the result of receiving a registration request message from a proxy filter (303) (1000); as the result of visiting the Email Rating Service's website (200) and learning about the email registry service (201); by being referred by other users of the service, or; simply as the result of conducting web based searches of the Internet in search of spam filtering solutions.

Since spammers typically use invalid and randomly generated email addresses in the "From" and "Reply-To" fields of the message header, the process to register an email address is designed to only allow one valid email address to be manually registered at a time, with each email address validated using a double opt-in process that requires the address owner to respond to an email message sent to the registered address by going to a web page and providing a randomly generated registration code that was included in the email message. A complete description of the entire process follows.

Each registration page is automatically generated on demand by the web server and includes: 1.) a non-machine readable registration code (typically in the form of a graphic image) that includes a randomly generated series of alphanumeric characters (506); 2.) a field for the user to enter the email address that they wish to register, and; 3.) a selection of radio buttons that allows the user to choose one option that describes the "type" of email that is typically sent using the entered email address. Email types may include (but are not limited to): 1.) Personal email messages -- low

volume personal and business email messages sent by a single person to friends, acquaintance or business associates; 2.) opt-in email messages -- bulk email that is sent to individuals who have agreed or "opted" to receive unscheduled or scheduled promotional or informational email from the owner of the email address; 3.) discussion list messages ("ListServs") -- email that is sent to individuals who have subscribed to receive emails of messages posted to a discussion list by other subscribers the list; 4.) regularly scheduled information services -- email messages that are sent to individuals who have agreed (either directly or indirectly) to receive email messages from the email address owner at some pre-defined regular interval. Examples would include monthly newsletters, scheduled service status reports, monthly billing notices, etc., and; 5.) irregularly scheduled information services -- email messages that are sent to individuals who have agreed (either directly or indirectly) to receive email messages from the address owner at random and un-scheduled intervals. Examples would include occasional newsletters, unscheduled service status reports, appointment reminder notices, etc.

After the user has completed and submitted the email address registration application page, the process continues by comparing the non-machine readable registration code entered by the user with the value represented by the graphically displayed alphanumeric code. (512) If the entered code does not match the graphically displayed alphanumeric code, then the process checks to see if the user has attempted to register the same email address with an incorrect registration code more than x times, where x is an integer equal to a value set by the system administrator. (207) (527) If the user has attempted to register the same email address with an incorrect registration code less than x times, then the process displays a registration failure message and a new, blank registration application page is generated with a newly generated non-machine readable registration code. (524) If the user has attempted to register the same email address with an incorrect registration code more than x times, then the process displays a registration failure message and advises the user that they will not be able to re-attempt registering that particular email address for a random period of time and returns the user to the main page of the website. (530) The objective of this process is to prevent a user from designing automated email address registration processes.

If the entered registration code does match the graphically displayed alphanumeric code (512) then the process continues by checking to see if the email address has already been registered. (515) If the email address has already been registered, then the process displays a message advising the user

that the email address has been registered (533) and asks the user if they would like to register a different address. (536) If an application to register the email address has already been submitted, but the email address has not yet been "validated" (518) (the address owner has confirmed that they wish to have the email address registered), then a message is displayed (521) telling the user that the address has already been submitted for registration but has not yet been validated by the address owner. The user is then asked if they would like to have another registration confirmation email message sent to the email address. (560)

If the email address has not been registered and there is no application for registration on file, then the system creates a randomly generated alphanumeric code that is saved with the email address in the Registry's database (206). In one embodiment of the invention the code and the email address are encrypted and included in a coded web page URL. The URL is then emailed to the address that was entered on the registration web page. (542) When the owner of the email address receives the message they are instructed to click on or cut and paste the URL into their web browser. The web page that the URL points to includes a server-based, automatic process that extracts the randomly generated alphanumeric code and encrypted email address from the URL and compares them to the information that was saved in the Registry database (206) when the application for registration was submitted. If both the alphanumeric code and email address from the URL match the alphanumeric code and email address in the Registry database, (206) (551) then the address has been confirmed as valid and recorded as fully registered by the address owner (572) in the Registry database. (206)

If the email that was sent to the email address provided during the application process bounces (returned as an invalid address), (548) then the database (206) entry for that email address is flagged as invalid. (569) If more than x days, where x is equal to an integer value configured by the system administrator (207) elapses without a response from the address owner, (554) then the database (206) entry is updated to indicate that the validation process failed due to a lack of response from the address owner. (557)

Once the email address has been validated by the address owner and added to the Registry database (206), (572) the address is then added (575) to the rating queue (205) (1600) for evaluation and a spam rating assignment. After the address has been evaluated and rated it is then added (578) to the ratings server (202). If the owner of the address requested that they be advised of the rating assigned

to their submitted email address, then the process will conclude by preparing and sending an email message with the assigned rating value (581) and explanation of what the rating means to the email address owner.

Fig. 7 describes the process that a user would use to create and maintain a personal GOlist. A GOlist is a list of email addresses that the user is prepared to always receive email from. This could include friends, relatives, business associates, customers, etc. The creation and use of a personal GOlist is completely optional and simply provides the user with more control over what email is delivered to their inbox. In the preferred embodiment of the invention the user can choose to create or add email addresses to their personal GOlist using an import function (610) that will allow the user to import email addresses from existing address books, text files, databases, or from another users GOlist. (635) Alternatively, (615) they could simply manually add email addresses to their personal GOlist. (640) Additional options (620, 625) are provided that allows the user to manually edit (645) and delete (650) email addresses from their personal GOlist. All GOlist adds and edits are evaluated (630) to ensure that none of the email addresses appear in both the users GOlist and STOPlist. If the same address appears in both lists, then a process is started that allows the user to resolve the conflict. (655)

Reciprocally, Fig. 8 describes the process that a user would use to create and maintain a personal STOPlist. A STOPlist is a list of email addresses that the user never wants to receive email from. The creation and use of a personal STOPlist is completely optional and simply provides the user with more control over what email is blocked from their inbox. In the preferred embodiment of the invention the user can choose to create or add email addresses to their personal STOPlist using an import function option (710) that will allow the user to import email addresses from existing address books, text files, databases, or from another users STOPlist. (735) Alternatively (715) they could simply manually add email addresses to their personal STOPlist. (740) Additional options (720, 725) are provided that allows the user to manually edit (745) and delete (750) email addresses from their personal STOPlist. All STOPlist adds and edits are evaluated (730) to ensure that none of the email addresses appear in both the users STOPlist and GOlist. If the same address appears in both lists, then a process is started that allows the user to resolve the conflict. (755)

Fig. 9 illustrates processes that are invoked each time that the user adds, removes or modifies email addresses in their personal GOlist or STOPlist. (760) If there are email messages in the users detained message list (106, 306) with email addresses that are also in the users GOlist or STOPlist, (765) then the proxy (102, 302) will determine if the disposition of these messages has changed as the result of the changes made to the users GOlist or STOPlist, (790) and whether the detained messages should be retrieved from the users ESP and forwarded to the users inbox (if the email address has been added to the GOlist), or deleted from the users detained list and ESP if the email address has been added to the users STOPlist and the user has configured the proxy (102, 302) to automatically delete all messages from senders whose address is in their personal STOPlist.

Additionally a process is started that will send the email addresses (775) that have been added to or removed from a users GOlist and STOPlist to the Registry database (206) along with the GUID for that users proxy installation. (102, 302) The Registry (201) in turn records when each email address has been added or removed from the GOlist or STOPlist related to that installation GUID. The number of GOlists and STOPlists that each email address is on and when the email address was added or removed from these lists can provide important information that is used by the CRP.

Turning now to Fig. 10 we can step through the process used by the proxy (102, 302) to retrieve a message from the users ESP and determine the current rating (if any) and disposition of the message. In one embodiment of the invention, the preferred email client (301) used by the receiver of the email message initiates a check for new email. (803) The proxy (302) will intercept the email check request and submit a request for just the header portion of new email messages to the users ESP on behalf of the users preferred email client (301). (806) After downloading all new email headers the proxy (302) will select the next message header from the downloaded list of message headers and attempt to parse out a valid email address for the sender of the email. (809) In the majority of cases this address can be found in the one of the three industry standard header fields as currently defined by RFC 2822 (Network Working Group, Request for Comments: 2822, April 2001, "Internet Message Format") and includes: 1.) From; 2.) Sender; and 3.) Reply-To: fields. In cases where there are multiple fields to choose from, each with a different email addresses, then the proxy (302) will comply with RFC 2822's recommendations for the automatic use of the From, Sender, and Reply-To fields.

Email based mailing lists may use additional industry standard header fields as currently defined by RFC 2369 (Network Working Group, Request for Comments: 2369, July 1998, "The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields") that identify the administrator of the mailing list that administrative email messages should be sent to, rather than the From or Reply-To addresses which may result in the message being redistributed to all of the subscribers of the mailing list in cases where the mailing list is configured as an interactive and un-moderated mailing list. To accommodate mailing lists, the proxy (102, 302) will also look and use the email address contained in the RFC defined "List-Owner" field in the message header. While a standard exists for mailing list email header fields, the use of the standard List-Owner field is only recommended, not required by the currently defined RFC for mailing list commands and header fields. As a result many mailing list software programs support and use a variety of custom field names to identify the list owner. To accommodate non-standard fields, the proxy (102, 302) will also look for non-standard list owner fields using an up-dateable list of known list owner fields that are in common use.

If the proxy (302) is unable to identify a valid email address for the sender or list owner (812) then depending on how the receiver has configured the proxy (302), (821) the email message is: 1.) retrieved from the users ESP and forwarded to the users preferred email client (301) (818), or; 2.) the proxy (302) places the message header for the email message in the receivers detained message list (306) so that the receiver can decide if they wish to retrieve or delete the message (824), or; 3.) the proxy (302) deletes the message headers for the email message and sends instructions to the ESP to delete the message.

If the proxy (302) is able to parse out a valid email address from the sender or list owner, it then checks to see if there are other messages with the same address in the receiver's detained list. (306) (815) If there are, then the message header is placed in the detained list. (306) (824) If there are no other messages with the same address in the users detained list, then the proxy (302) checks to see if the senders email address is on the receivers personal GOlist. (830) If the email address is on the receivers GOlist, then the entire message is retrieved from the receivers ESP and forwarded to the receivers preferred email client (301). (848) If the senders email address is not on the receivers GOlist, then the proxy (302) checks the receivers STOPlist. (833) If the senders email address is on the receivers STOPlist, then depending on how the receiver has configured the proxy (302) (857),

the message headers are placed on the receivers detained list for review by the receiver (860), or the proxy (302) deletes the message header (851) and instructs the receivers ESP to delete the message. (854)

If the email address is not on the users STOPlist (833), then the proxy (302) sends a request to the ratings server (202) for the current spam rating of the email address. (836) If the ratings server (202) does not reply to the rating request after x number of tries (839), then depending on how the receiver has configured the proxy (302) (842) the email message is either retrieved from the receivers ESP and forwarded on to the receivers preferred email client (301) (892), or the message headers are placed on the receivers detained list (306) with a note that the email was detained because the proxy (302) was unable to contact the ratings server. (202) (845)

If the ratings server (202) sends a reply to the rating request, the proxy (302) evaluates the reply to determine what action to take based on the rating value provided. If the returned rating indicates that the address is unknown to the Registry (201), or that the address is in the Registry (201) but a registration request needs to be sent to the owner of the email address (863), then the receivers proxy (302) launches the registration request service (307) (872) and emails a registration request message to the sender. If there is no rating value returned by the ratings server (202) (864), the proxy (302) places the message headers on the receivers detained message list (306) (875) and then checks to see if there are additional headers to process. (827)

If a rating value is returned by the ratings server (202), the proxy (302) evaluates the rating to determine how to handle the message. If the rating is equal to or below the receiver's minimum acceptable rating value, the proxy (302) retrieves the entire message from the receivers ESP and forwards it to the receivers preferred email client (301) (878) and deletes the header from the downloaded header list. (881) If the returned rating is above the receivers minimum acceptable rating value, and if the receiver has configured the proxy (302) to delete email messages with address ratings above their minimum acceptable rating value (869), then the proxy (302) instructs the ESP to delete the message (887) and deletes the message header from the downloaded header list. (890) Finally if the receiver has configured the proxy (302) not to delete messages with rating values above their minimum acceptable rating value, then the message header is placed on the

receivers detained list with an indicator showing that the returned rating value was above the receivers minimum acceptable rating value. (884)

Email registration requests are only sent to senders who have sent the receiver a message and only by the receiver's proxy (302) when instructed to do so by the Registry (201). Fig. 13 illustrates registration request process that is . Before sending out a registration request message to a sender, the registration request module (307) checks to see if a registration request message has been sent to the sender within the last x days, where x is equal to a value defined by the receiver. (900) If a registration request has been sent out to the sender within the past x days, then the process ends. If no registration request have been sent by the registration request module (307) to the sender, then the registration request module (307) checks to see if the email message that the was received from the sender was passed on to the receivers inbox or placed in the detained message list (306). (905) If the message was passed on to the receiver's inbox, then the registration request module (307) generates a registration request message using a message that has been pre-defined by the receiver that advises the sender that their message has been delivered to the receiver's inbox, but their email address has not yet been registered and that they should consider registering their email address with the email rating service. (200) (930) A URL for the registration page is included in the message. If the message was placed in the receivers detained message list (306), then the registration request module (307) generates a registration request message using a message that has been pre-defined by the receiver that advises the sender that their message has not been delivered to the receiver's inbox and that the delivery of their message is not guaranteed unless they register their email address with the email rating service. (200) (910) A URL for the registration page is included in the message.

In one embodiment of the invention the receiver is able to personalize registration request messages that are sent out to senders, however the inclusion of some elements in the registration request message will be required to ensure the integrity of the process. These elements may include, the URL of the registration page, details about the email rating service, privacy policy statements, etc.

Once the registration request module (307) has emailed the registration request message to the sender it advises the Registry (201, 210) of the email address that the message was sent to (915) and the date and time that the message was sent on. (920)

The registration request module (307) continues to monitor incoming email messages for bounced registration requests. (925) If a registration request bounces, then the registration request module (307) updates all of the message headers from the bounced email address in the detained list (306) to indicate that email from that address is possibly spam. (935) The registration request module (307) also advises the Registry (201, 210) of all bounced registration requests. (940)

Email addresses that need to be rated or re-rated by the CRP are prioritized and submitted to a "rating queue". (205) In the preferred embodiment of the invention an evaluation priority may be automatically or manually assigned to each email address. Email addresses are evaluated in ascending order of priority using a First In, First Out (FIFO) arrangement.

In one possible embodiment an evaluation priority scale of 1 to 10 may be used, where 1 equals the highest priority and 10 equals the lowest priority. In this embodiment if 15 email address were in the queue with an evaluation priority value of 1, and 35 email address were in the queue with an evaluation priority value of 6, and 126 email addresses where in the queue with an evaluation priority value of 8, then all of the priority 1 email addresses would be evaluated in ascending date/time order, followed by all of the priority 6 email addresses in ascending date/time order, followed by all of the priority 8 email addresses in ascending date/time order. If additional email addresses with higher evaluation priority values are added to the queue while lower priority email addresses are being evaluated, then the next address to be evaluated will be the address with the higher evaluation priority value and the oldest date/time stamp. In addition, rules driven processes may re-define the priority evaluation value assigned to any email address already submitted to the rating queue (205) at any time resulting in an email address being assigned a higher or lower evaluation priority value. Email addresses that are added to the queue with no evaluation priority are automatically assigned the lowest evaluation priority by the queue management process. (205)

In the preferred embodiment of the invention email evaluation priority values may be automatically or manually determined by the way that each email address is submitted to the queue. Submission methods may include, (but are not limited to): 1.) email addresses that are added to a users GOlist; 2.) email addresses that are added to a users STOPlist; 3.) email addresses that are provided by the address owner through the registration process; 4.) email address that are submitted by a rule; or 5.) email addresses that are manually submitted to the queue. In the case of submission methods 1,2,

and 3 the evaluation priority may be pre-determined by the system administrator (207) and automatically assigned by the queue submission process. In the case of submission method 4, the evaluation priority may be automatically determined by the rule that submitted the email address to the queue for evaluation. And in the case of submission method 5, the evaluation priority may be manually assigned by the user who submitted the email address to the queue.

Date/time ranges that define when the address should be processed may also be provided for each address added to the queue. Addresses with specified date/time processing ranges are not processed, regardless of their evaluation priority assignment until the defined date/time range. During the defined date/time range for processing the priority value assigned to the address (if any) are used to determine when the address is processed. As the time period comes closer to expiring, the evaluation priority of the address will increase to ensure that the address is evaluated within the specified date/time range.

Email rating values are assigned to each address using a series of pre-defined "collaborative rules". Any number of rules may be defined, and one or more rules may be used to determine an address's current rating value. Rules are collaborative in nature in that they use information that is provided directly and indirectly by the senders and receivers of email messages, along with operational information that is derived from the process of users sending and receiving email messages and maintaining their personal proxy software. (102, 302)

Information about each email address that is directly provided by users may include (but is not limited to): 1.) The type of email that is typically sent from the users registered email address as previously described, and; 2.) spam complaint submissions.

Information about each email address that is indirectly provided by users may include (but is not limited to): 1.) Email addresses and the date/time stamp that each email address was added to or removed from a users GOlist; 2.) email addresses and the date/time stamp that each email address was added to or removed from a users STOPlist; 3.) header information from email messages processed by the proxy (102, 302); 4.) the IP address of the registrant at the time they registered their email address; 5.) the HTTP header information from the registrants browser at the time they registered their email address; 6.) the date/time that the email address was registered; 7.) date/time stamp and the senders email address for each email header that is deleted from a users detained

message list (106, 306) by the user, and; 8.) date/time stamp and the senders email address for each email header that is deleted from a users detained message list (106, 306) by an auto delete function.

Information about each email address that is derived from operational activities may include (but is not limited to): 1.) How the email address was added to the Registry (201). I.e.: By the owner, from a personal GO/STOPlist, etc.; 2.) the date/time stamp each time that an email address's status and rating information was requested by a proxy (102, 302); 3.) a complete history of all rating changes for each email address, including the date/time stamp of each rating change and the new rating; 4.) the number of registration requests that were sent to the address owner before the owner registered the address; 5.) the time elapsed between the time that the user submitted a registration application form and the time that they validated the address; 6.) the number of times that the registration process "timed out" (the address owner did not respond to the validation request within the administrators (207) pre-set period of time) requiring the address owner to re-start the registration process.

Information that is not used in any way to calculate email address ratings includes: 1.) The body text of email messages, and; 2.) any information that could personally identify the sender or receiver of the email message.

In the preferred embodiment of the invention rating rules can be created, added, changed, suspended or deleted at any time. Rating rules are applied using a high level scripting language that: 1.) Allows rating rules to be invoked in a specific order; 2.) allows rating rule scripts to be chained so that a rule or script can invoke another script; 3.) allows rating rules or rating rule scripts to invoke one or more additional rating rules or rating rule scripts based on the results produced by the invoking rating rule or rating rule script; 4.) allows subsequently run rating rules or rating rule scripts to use the results from one or more previously run rating rules or rating rule scripts; 5.) allows ratings rules or rating rule scripts to be results driven so that the product of each rating rule within the script will determine what rule will be invoked next; 6.) allow rating rules or rating rule scripts to be invoked based upon a predefined schedule; 7.) allow rating rules or rating rule scripts to be invoked based upon a predefined set of circumstances such as a system restart, pre-determined number of email addresses waiting in the rating queue (205) for processing, etc.; 8.) allow rating rules or rating rule scripts to re-add an address to the rating queue (205) and specify an evaluation priority and date/time range

that the address should be re-rated using a specific rating rule or rating rule script; 9.) allows the wildcard selection of email addresses to be evaluated by a rule, i.e.: select and evaluate all email addresses that end with "someplace.com"; 10.) allow the use of include files (lists) of email addresses that are to be evaluated by a rule, and 11.) allow variables used by each rule to be specified by the creator of the script or by the results of previously run rating rule scripts or rating rules.

In addition to the definition of and ad-hoc use of rating rule scripts, the system administrator (207) is also able to associate rating rules or rating rule scripts with each email address when the email address is added to the rating queue (205). What rating rules and rating rule scripts are associated with the email address can depend on how the email address was added to the rating queue. (205) I.e.: it was added to a users GOlist or STOPlist and has not yet been rated, it was added to the Registry (201) by the address owner, etc.)

If an email address is manually added to the rating queue (205) by an administrator (207), the administrator (207) has the option to specify what rating rules or rating rule scripts are to be used for evaluating the email address, the evaluation priority of the email address, and any pre-defined schedules or time ranges during which the address should be evaluated.

Rating rules contain a series of mathematical, Boolean and procedural instructions that are designed to generate a Contributory Rating Value ("CRV") using direct, indirect or derived information about the email address as previously described. In the preferred embodiment of the invention CRVs are floating-point numbers of any value. The CRV generated by each rule only "contributes" to the final rating value assigned to each email address evaluated by the rule. They are not the actual rating values assigned to the email address. It should also be noted that rules may be created to generate negative CRVs, zero and positive CRVs, or negative, zero and positive CRVs.

Negative CRVs represent a relative level of improvement over previously generated CRVs by the same rule, where larger negative values represent the most improvement, and smaller negative values represent the least improvement. Zero and positive values represent absolute spam CRVs that are based upon currently available direct, indirect and/or derived information for the email address, where 0 means that the rule is unable to detect any evidence of spamming whatsoever, and larger

values represent increasingly stronger evidence that the email address is being used to send unwanted email.

In one embodiment of the invention values assigned to each email address that represent the current rating would be a series of integers from 0 to 9. Where 0 means that it is extremely unlikely that email received from the address is spam, and 9 means that it is extremely likely that email received from the email address is spam.

In instances where only a single rule has been used to evaluate an email address, only zero and positive CRV results are used to generate the current rating value of the address by rounding down the CRV to the nearest integer and assigning the integer as the current rating value for the email address. If the resulting integer is greater than 9, then 9 becomes the assigned rating value.

In instances where multiple rules are used to evaluate the email address during a single evaluation session, the session will sum and average all of the generated CRVs (negative and positive) for the session, round down and convert the resulting floating point value to an integer, which becomes the final rating value for the email address. If the email address had a pre-assigned rating value, that value may or may not be included in the sum and averaging functions. If the resulting integer is greater than 9, then 9 becomes the assigned rating value. If the resulting integer is less than 0, than 0 becomes the assigned rating value

While any number of rules can be created and used to evaluate and rate email addresses, for the purposes of illustration we will describe three rules that could be considered the minimum needed to accurately assess and rate an email address. The following examples are only provided to illustrate how rules may work in one possible embodiment of the invention and should not be considered as functionally complete. In addition, the sample rules provided only illustrate the generation of positive CRVs. Variations of these example rules could generate negative CRVs to account for users who are trying to improve or correct their rating assignment by implementing email best practices. As experience is gained in the creation and deployment of rating rules, more sophisticated and functionally complete rules will be developed.

Sample Rule #1 - Excessive Rating Requests: This rule assumes that if the ratings server (202) receives an excessive number of rating requests for an email address over a pre-defined period of

time, that there is a possibility that the address is being used to send spam. This rule only generates zero and positive CRVs. When run, the rule queries the email database (206) for all rating requests received for the email address being evaluated since the last time that the rule was used to evaluate the same address. The rule also queries the email database (206) and calculates an average value for all rating requests received for all email addresses that are of the same type as the email address being evaluated and with a currently assigned spam rating value of x or less, where x is a value assigned by the system administrator (207). The number of rating requests received for the email address being evaluated is subtracted from the average number of email rating requests received for the comparative email addresses. The difference is then multiplied by x (where x is a value defined by the administrator (207)) to arrive at a CRV that is used to calculate the final rating assignment for the email address when all other rules have completed their evaluation of the address.

Rule #1 Example: someone@somewhere.com is a personal address that has a rating value of 1 currently assigned to it. The last time that the address was evaluated by the Excessive Rating Requests rule it was re-added to the rating queue (205) with instructions to re-evaluate the address within 15 to 30 minutes using the same rule with an evaluation priority of 4. After 15 minutes has elapsed the queue starts the revaluation process of someone@somewhere.com using the Excessive Rating Requests rule and determines that the email address has received 13 rating requests in the past 15 minutes. The rule queries the email database (206) and determines that the average number of requests received for the same type of email address (personal) with a current rating assignment of 2 or less in the past 15 minutes is 4.3, giving us a difference between the average number of rating requests received by other email addresses and the number of rating requests received for someone@somewhere.com of 8.7. The administrator (207) has assigned a multiplier value of .5, which results in a final CRV of 4.35. If no other rules have been used to evaluate the email address, then the process continues by averaging the currently assigned rating value of 1 with the CRV of 4.35 to arrive at an average value of 2.675 which when rounded down to the nearest integer results in a new rating value of 2, which is the new rating value assigned to someone@somewhere.com. The process concludes by comparing the previously calculated rating value for someone@somewhere.com with the value previously generated by the same rule. Since the rating value has increased by 1, the rule re-submits the email address to the rating queue (205) with a evaluation priority of 8 and a request a review of the email address using the same rule in not more

than 15 minutes and not less than 30 minutes from the time it was submitted to the rating queue (205).

Sample Rule #2 - Excessive STOPlist Assignments: This rule assumes that if an email address is assigned to an excessive number of user STOPlists, that there is a possibility that the address is being used to send spam. This rule generates zero and positive CRVs. When run, the rule queries the email database (206) for a total count of STOPlists that the email address is currently assigned to by users of the proxy (102, 302) software. The rule also queries the email database (206) for all email addresses that are currently assigned to one or more user STOPlists and calculates the average number of STOPlists that other email addresses are on. The average number of STOPlists that other email addresses are on is subtracted from the number of STOPlists that the email address that is being evaluated is on. If the difference is not equal to or less than 0, then the difference is multiplied by x (where x is a value defined by the administrator (207)) to arrive at a CRV that is used to calculate the final rating value assignment for the email address when all other rules have completed their evaluation of the address.

Rule #2 Example: someone@somewhere.com is a personal address that has a rating value of 2 currently assigned to it. The last time that the address was evaluated by the Excessive STOPlist Assignment rule it was re-added to the rating queue (205) with instructions to re-evaluate the address within 6 to 10 hours using the same rule. After 6 hours has elapsed the queue starts the revaluation process of someone@somewhere.com using the Excessive STOPlist Assignments rule and determines that the email address is currently on 37 STOPlists. The rule queries the email database (206) and determines that the average number of STOPlists that other addresses of the same type (personal) are on is 5.8, giving us a difference between the average number of STOPlists that other email addresses are on and the number of STOPlists that someone@somewhere.com is on of 11.2. The administrator (207) has assigned a multiplier value of .5, which results in a final CRV of 5.6. If no other rules have been used to evaluate the email address, then the process continues by averaging the currently assigned rating value of 2 with the CRV of 5.6 to arrive at an average value of 3.8 which when rounded down to the nearest integer results in a new rating value of 3, which is assigned to someone@somewhere.com. The process concludes by comparing the previously calculated rating value for someone@somewhere.com with the value previously generated by the same rule. Since the rating value has increased by 1, the rule re-submits the email address to the

rating queue (205) with a evaluation priority of 5 and requests a review of the email address using the same rule in not more than 6 hours and not less than 10 hours from the time it was submitted to the rating queue (205).

Sample Rule #3 - Excessive Complaints: This rule assumes that if an email address receives an excessive number of complaints from users about email being sent from the address, that there is a strong possibility that the address is being used to send spam. This rule generates zero and positive CRVs. When run, the rule queries the email database (206) for a total count of complaints received from users for the email address being evaluated. The rule also queries the email database (206) for email addresses of the same type, that have received one or more complaints, and that have a currently assigned rating value of x or less, where x is an integer value assigned by the system administrator. (207) The process then uses the query results to calculate a value that represents the average number of spam complaints received for all other email addresses that complaints have been received for. The average number of complaints received for other email addresses are subtracted from the number of complaints received from the email address that is being evaluated. If the difference is greater than 0 than the difference is multiplied by x where x is a value defined by the administrator (207) to arrive at a CRV that is used to calculate the final rating value assignment for the email address when all other rules have completed their evaluation of the address.

Rule #3 Example: someone@somewhere.com is a personal address that has a rating value of 4 currently assigned to it. The last time that the address was evaluated by the Excessive Complaints rule it was re-added to the rating queue (205) with instructions to re-evaluate the address within 4 to 5 hours using the same rule. After 4 hours has elapsed the queue starts the revaluation process of someone@somewhere.com using the Excessive Complaints rule and determines that the email address has received a total of 28 complaints. The rule queries the email database (206) and determines that the average number of complaints received by other addresses of the same type (personal) is 3.21, giving us a difference between the average number of complaints that other email addresses have received and the number of complaints that someone@somewhere.com has received of 24.79. The administrator (207) has assigned a multiplier value of .5, which results in a final CRV of 12.395. If no other rules have been used to evaluate the email address, then the process continues by averaging the currently assigned rating value of 3 with the CRV of 12.395 to arrive at an average value of 7.6975 which when rounded down to the nearest integer results in a new rating value of 7,

which is assigned to someone@somewhere.com. The process concludes by comparing the previously calculated rating value for someone@somewhere.com with the value previously generated by the same rule. Since the rating value has increased by 4, the rule re-submits the email address to the rating queue (205) with a evaluation priority of 9 and requests a review of the email address using the same rule in not more than 1 hour and not less than 2 hours from the time it was submitted to the rating queue (205).

Fig. 1

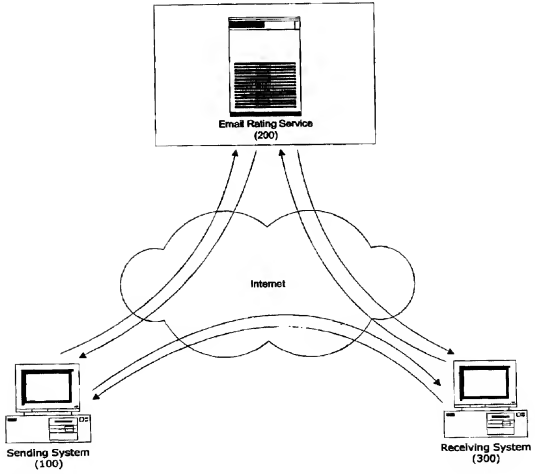

Email Rating Service
(200)
Internet
Sending System
(100)
Receiving System
(300)

Fig. 2

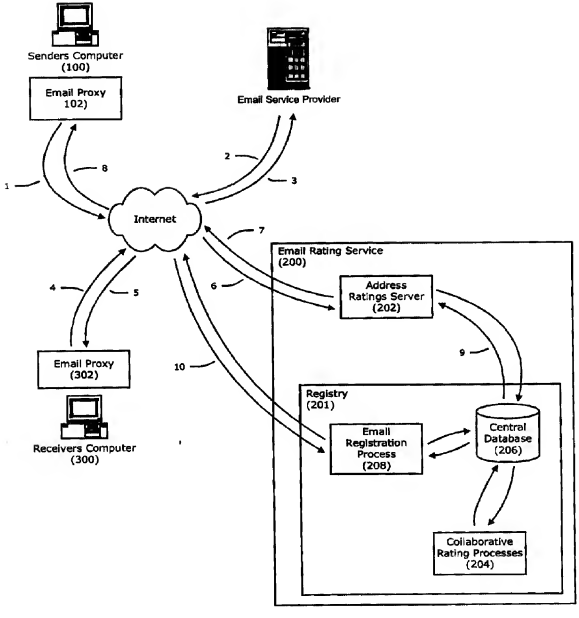

Senders Computer
(100)
Email Proxy
102)
Email Service Provider
1
2
3
8
Internet
7
Email Rating Service
(200)
4
5
6
Address
Ratings Server
(202)
9
Email Proxy
(302)
10
Registry
(201)
Email
Registration
Process
(208)
Central
Database
(206)
Receivers Computer
(300)
Collaborative
Rating Processes
(204)

Fig. 3

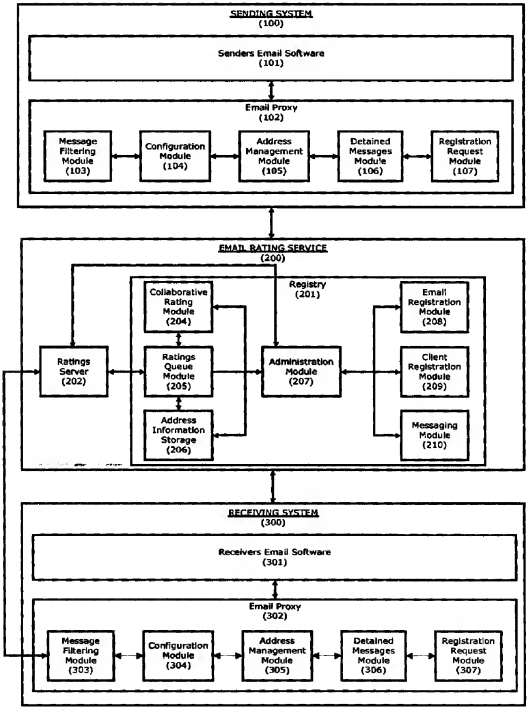

SENDING SYSTEM
(100)
Senders Email Software
(101)
Email Proxy
(102)
Message Filtering Module (103)
Configuration Module (104)
Address Management Module (105)
Detained Messages Module (106)
Registration Request Module (107)
EMAIL RATING SERVICE
(200)
Registry
(201)
Collaborative Rating Module (204)
Email Registration Module (208)
Ratings Server (202)
Ratings Queue Module (205)
Administration Module (207)
Client Registration Module (209)
Address Information Storage (206)
Messaging Module (210)
RECEIVING SYSTEM
(300)
Receivers Email Software
(301)
Email Proxy
(302)
Message Filtering Module (303)
Configuration Module (304)
Address Management Module (305)
Detained Messages Module (306)
Registration Request Module (307)

Fig. 4

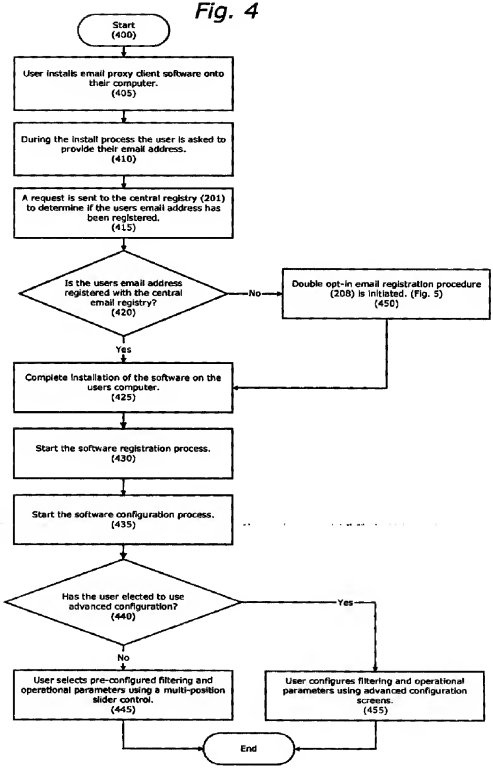

Start
(400)
User installs email proxy client software onto their computer.
(405)
During the install process the user is asked to provide their email address.
(410)
A request is sent to the central registry (201) to determine if the users email address has been registered.
(415)
Is the users email address registered with the central email registry?
(420)
No
Double opt-in email registration procedure (208) is initiated. (Fig. 5)
(450)
Yes
Complete installation of the software on the users computer.
(425)
Start the software registration process.
(430)
Start the software configuration process.
(435)
Has the user elected to use advanced configuration?
(440)
Yes
No
User selects pre-configured filtering and operational parameters using a multi-position slider control.
(445)
User configures filtering and operational parameters using advanced configuration screens.
(455)
End

Fig. 5

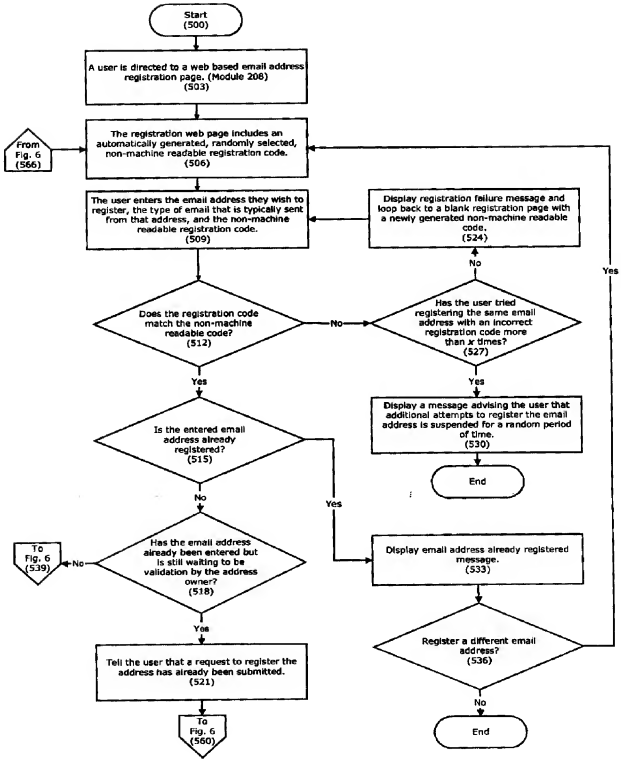

Start
(500)
A user is directed to a web based email address registration page. (Module 206)
(503)
From Fig. 6
(566)
The registration web page includes an automatically generated, randomly selected, non-machine readable registration code.
(506)
The user enters the email address they wish to register, the type of email that is typically sent from that address, and the non-machine readable registration code.
(509)
Display registration failure message and loop back to a blank registration page with a newly generated non-machine readable code.
(524)
No
Yes
Does the registration code match the non-machine readable code?
(512)
No
Has the user tried registering the same email address with an incorrect registration code more than x times?
(527)
Yes
Yes
Display a message advising the user that additional attempts to register the email address is suspended for a random period of time.
(530)
End
Is the entered email address already registered?
(515)
No
Yes
To Fig. 6
(539)
No
Has the email address already been entered but is still waiting to be validation by the address owner?
(518)
Display email address already registered message.
(533)
Register a different email address?
(536)
Yes
Tell the user that a request to register the address has already been submitted.
(521)
No
To Fig. 6
(560)
End

Fig. 6

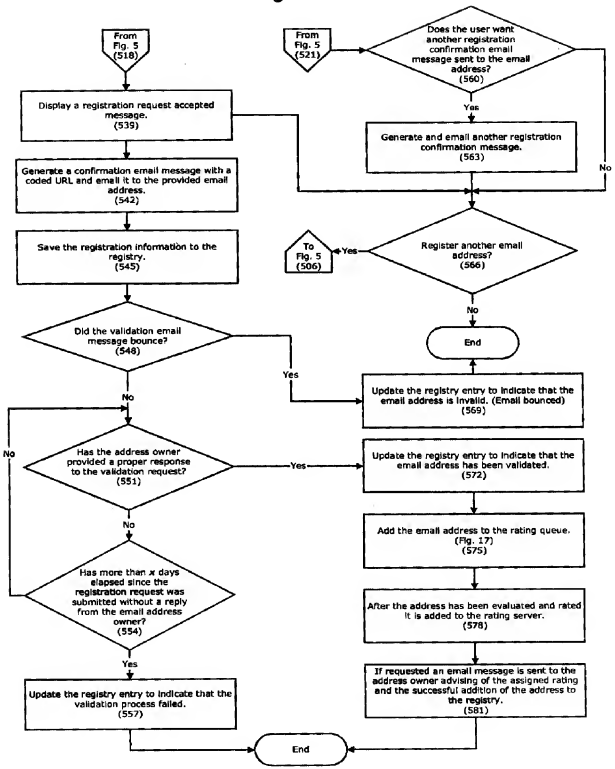

From Fig. 5 (518)
Display a registration request accepted message. (539)
Generate a confirmation email message with a coded URL and email it to the provided email address. (542)
Save the registration information to the registry. (545)
Did the validation email message bounce? (548)
Yes
No
Has the address owner provided a proper response to the validation request? (551)
No
Yes
Has more than x days elapsed since the registration request was submitted without a reply from the email address owner? (554)
No
Yes
Update the registry entry to indicate that the validation process failed. (557)
End
From Fig. 5 (521)
Does the user want another registration confirmation email message sent to the email address? (560)
Yes
No
Generate and email another registration confirmation message. (563)
To Fig. 5 (506)
Yes
Register another email address? (566)
No
End
Update the registry entry to indicate that the email address is invalid. (Email bounced) (569)
Update the registry entry to indicate that the email address has been validated. (572)
Add the email address to the rating queue. (Fig. 17) (575)
After the address has been evaluated and rated it is added to the rating server. (578)
If requested an email message is sent to the address owner advising of the assigned rating and the successful addition of the address to the registry. (581)

Fig. 7

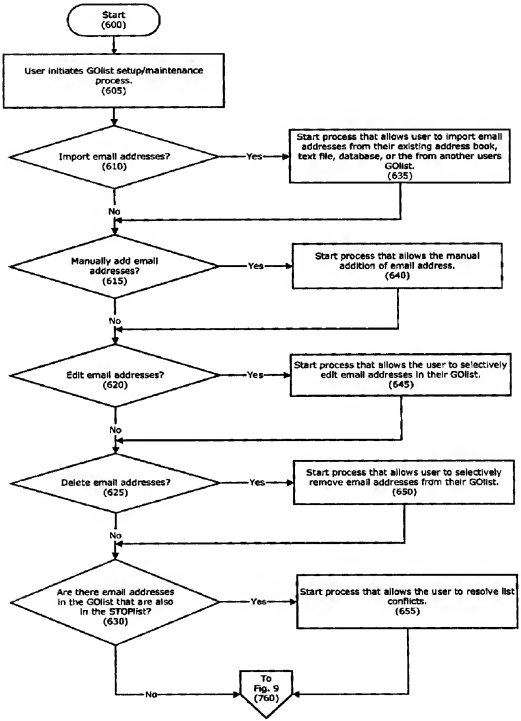

Start
(600)
User initiates GOlist setup/maintenance process.
(605)
Import email addresses?
(610)
Yes
Start process that allows user to import email addresses from their existing address book, text file, database, or the from another users GOlist.
(635)
No
Manually add email addresses?
(615)
Yes
Start process that allows the manual addition of email address.
(640)
No
Edit email addresses?
(620)
Yes
Start process that allows the user to selectively edit email addresses in their GOlist.
(645)
No
Delete email addresses?
(625)
Yes
Start process that allows user to selectively remove email addresses from their GOlist.
(650)
No
Are there email addresses in the GOlist that are also in the STOPlist?
(630)
Yes
Start process that allows the user to resolve list conflicts.
(655)
No
To Fig. 9 (760)

Fig. 8

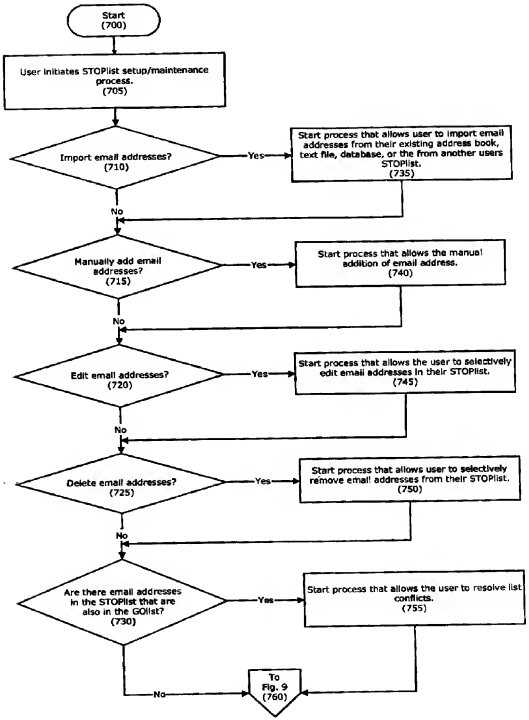

Start
(700)
User initiates STOPlist setup/maintenance process.
(705)
Import email addresses?
(710)
Yes
Start process that allows user to import email addresses from their existing address book, text file, database, or the from another users STOPlist.
(735)
No
Manually add email addresses?
(715)
Yes
Start process that allows the manual addition of email address.
(740)
No
Edit email addresses?
(720)
Yes
Start process that allows the user to selectively edit email addresses in their STOPlist.
(745)
No
Delete email addresses?
(725)
Yes
Start process that allows user to selectively remove email addresses from their STOPlist.
(750)
No
Are there email addresses in the STOPlist that are also in the GOlist?
(730)
Yes
Start process that allows the user to resolve list conflicts.
(755)
No
To Fig. 9 (760)

Fig. 9

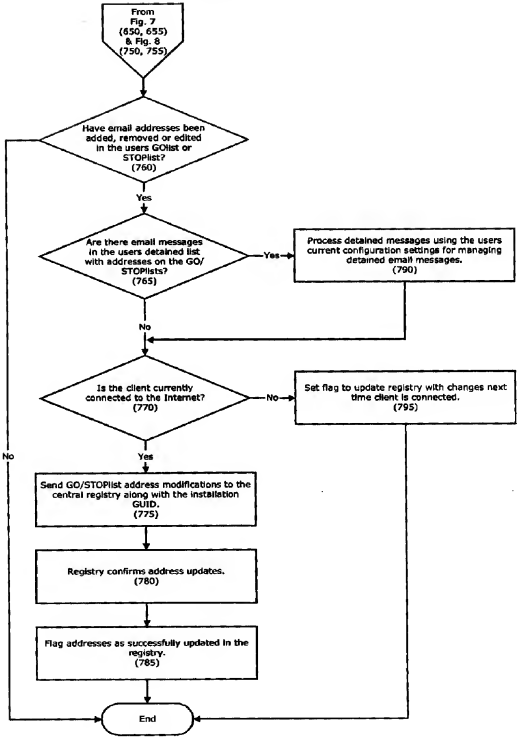

From Fig. 7 (650, 655) & Fig. 8 (750, 755)
Have email addresses been added, removed or edited in the users GOlist or STOPlist? (760)
Yes
Are there email messages in the users detained list with addresses on the GO/ STOPlists? (765)
Yes
Process detained messages using the users current configuration settings for managing detained email messages. (790)
No
Is the client currently connected to the Internet? (770)
No
Set flag to update registry with changes next time client is connected. (795)
No
Yes
Send GO/STOPlist address modifications to the central registry along with the installation GUID. (775)
Registry confirms address updates. (780)
Flag addresses as successfully updated in the registry. (785)
End

Fig. 10

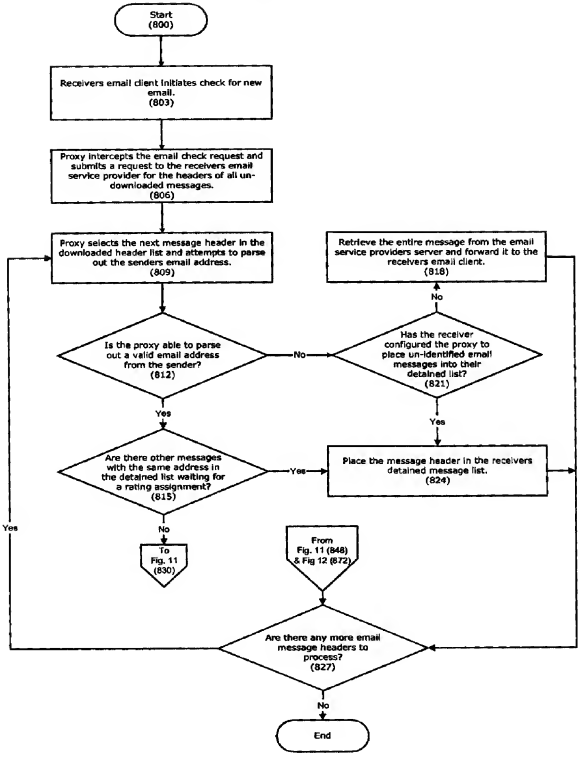

Start
(800)
Receivers email client initiates check for new email.
(803)
Proxy intercepts the email check request and submits a request to the receivers email service provider for the headers of all un-downloaded messages.
(806)
Proxy selects the next message header in the downloaded header list and attempts to parse out the senders email address.
(809)
Is the proxy able to parse out a valid email address from the sender?
(812)
No
Has the receiver configured the proxy to place un-identified email messages into their detained list?
(821)
No
Retrieve the entire message from the email service providers server and forward it to the receivers email client.
(818)
Yes
Yes
Are there other messages with the same address in the detained list waiting for a rating assignment?
(815)
Yes
Place the message header in the receivers detained message list.
(824)
No
To Fig. 11 (830)
Yes
From Fig. 11 (848) & Fig 12 (872)
Are there any more email message headers to process?
(827)
No
End

Fig. 11

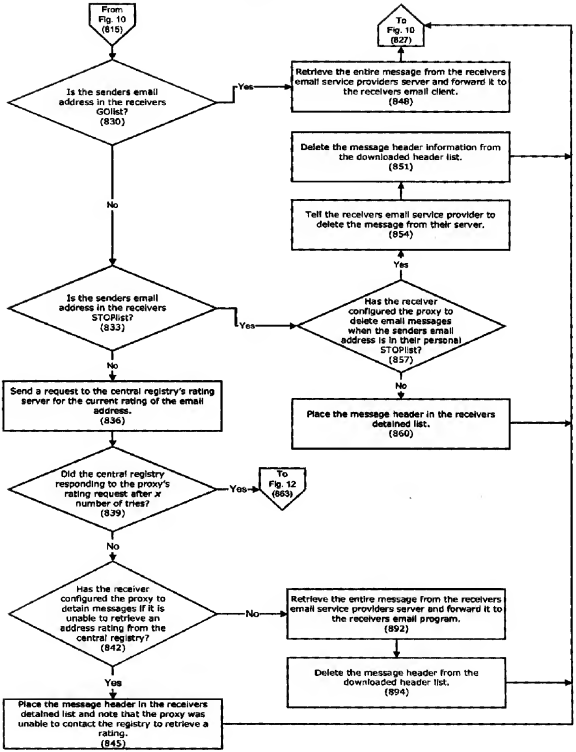

From Fig. 10 (815)
Is the senders email address in the receivers GOlist? (830)
Yes
No
Is the senders email address in the receivers STOPlist? (833)
Yes
No
Send a request to the central registry's rating server for the current rating of the email address. (836)
Did the central registry responding to the proxy's rating request after x number of tries? (839)
Yes
To Fig. 12 (863)
No
Has the receiver configured the proxy to detain messages if it is unable to retrieve an address rating from the central registry? (842)
No
Yes
Place the message header in the receivers detained list and note that the proxy was unable to contact the registry to retrieve a rating. (845)
To Fig. 10 (827)
Retrieve the entire message from the receivers email service providers server and forward it to the receivers email client. (848)
Delete the message header information from the downloaded header list. (851)
Tell the receivers email service provider to delete the message from their server. (854)
Yes
Has the receiver configured the proxy to delete email messages when the senders email address is in their personal STOPlist? (857)
No
Place the message header in the receivers detained list. (860)
Retrieve the entire message from the receivers email service providers server and forward it to the receivers email program. (892)
Delete the message header from the downloaded header list. (894)

Fig. 12

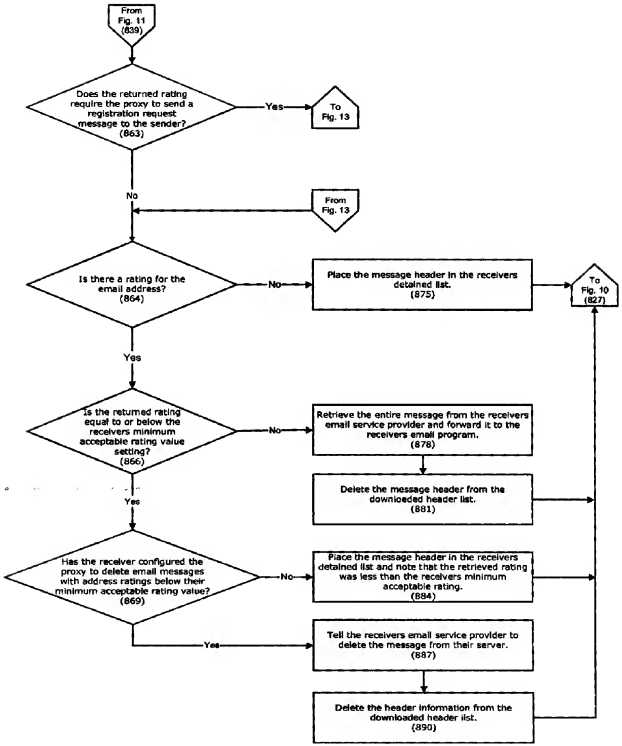
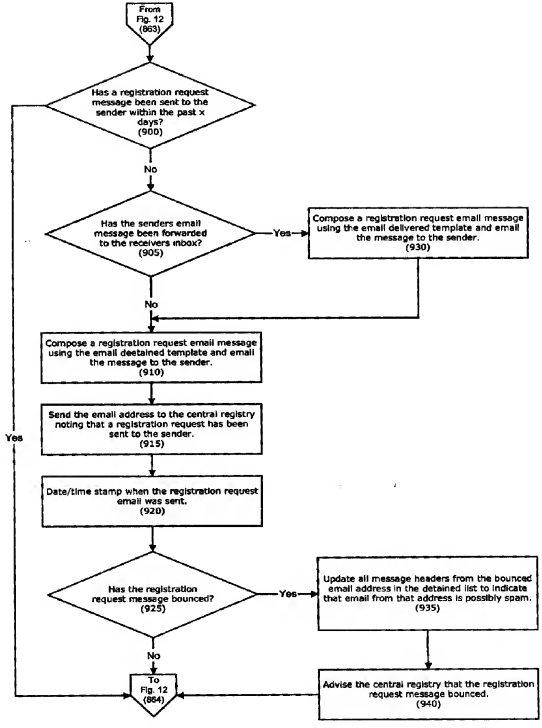

From Fig. 11 (839)
Does the returned rating require the proxy to send a registration request message to the sender? (863)
Yes
To Fig. 13
No
From Fig. 13
Is there a rating for the email address? (864)
No
Place the message header in the receivers detained list. (875)
To Fig. 10 (827)
Yes
Is the returned rating equal to or below the receivers minimum acceptable rating value setting? (866)
No
Retrieve the entire message from the receivers email service provider and forward it to the receivers email program. (878)
Delete the message header from the downloaded header list. (881)
Yes
Has the receiver configured the proxy to delete email messages with address ratings below their minimum acceptable rating value? (869)
No
Place the message header in the receivers detained list and note that the retrieved rating was less than the receivers minimum acceptable rating. (884)
Yes
Tell the receivers email service provider to delete the message from their server. (887)
Delete the header information from the downloaded header list. (890)

Fig. 13


From Fig. 12 (863)
Has a registration request message been sent to the sender within the past x days? (900)
No
Has the senders email message been forwarded to the receivers inbox? (905)
Yes
Compose a registration request email message using the email delivered template and email the message to the sender. (930)
No
Compose a registration request email message using the email deetained template and email the message to the sender. (910)
Send the email address to the central registry noting that a registration request has been sent to the sender. (915)
Yes
Date/time stamp when the registration request email was sent. (920)
Has the registration request message bounced? (925)
Yes
Update all message headers from the bounced email address in the detained list to indicate that email from that address is possibly spam. (935)
No
To Fig. 12 (864)
Advise the central registry that the registration request message bounced. (940)